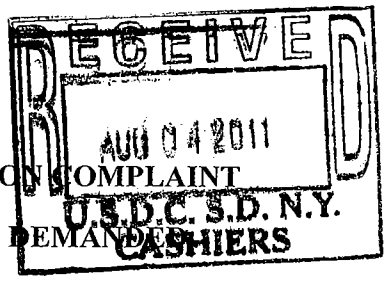
JUDGE KOELTL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

11 CIV 5436

BETSY FEIST, individually, and on behalf of all others similarly situated, Plaintiff, vs. RCN CORPORATION and PAXFIRE, INC., Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**



Plaintiff Betsy Feist brings this action individually and on behalf of: a) a class of persons who have had their Internet searches monitored, intercepted, manipulated and/or redirected via the use of Paxfire technology, including, but not limited to, the customers of the following Internet service providers: Cavalier, Charter, Cincinnati Bell, Cogent Communications, DirecPC, Frontier, Insight Broadband, Iowa Telecom, Defendant RCN, and Wide Open West, and any others to be determined in discovery (the "Paxfire Class");[1] b) a class of all RCN customers whose Internet searches were monitored, intercepted, manipulated and/or redirected (the "RCN Class"); and c) a class of all members of the RCN and/or Paxfire Classes who are citizens and/or residents of the state of New York (the "New York Class").

This case arises from Defendants' intentional and knowing interception of data intended for Yahoo!, Bing, or Google (the "Search Engines"), via use of hardware and/or software provided by Defendant Paxfire, as well as the monitoring, manipulation, aggregation, and/or marketing of that data. This interception was done secretly, without users' consent or knowledge, in violation of federal and state laws, and in breach of RCN's agreements with its customers. Plaintiff and the Classes seek damages and equitable relief.

Plaintiff alleges the following upon personal knowledge as to her own acts, and upon information and belief based on the investigation conducted by Plaintiff's counsel, including consultation with technology experts, as to all other matters.

NATURE OF THE ACTION

1. Defendants violated Plaintiff's privacy, and compromised her financial interests and computer security, by knowingly and intentionally intercepting her Internet communications in order to generate income for themselves. Rather than direct Plaintiff to the websites she

[1] The Internet service providers are herein referred to as "the ISPs."

actually requested, Defendants secretly gave her computer system false information that directed Plaintiff to websites that *looked* like the websites she intended to visit, but were actually controlled by and located on servers belonging to Defendant RCN and/or Defendant Paxfire. In other instances, when Plaintiff ran searches, Defendants directed Plaintiff through advertising affiliates onto third-party commercial web pages, rather than provide Plaintiff with the requested search results. Without Plaintiff's knowledge or consent, Defendants used Paxfire's hardware and/or software to misdirect Plaintiff to these servers; impersonate the websites Plaintiff wished to view; and monitor, manipulate, and/or monetize the searches run and page-visits made by Plaintiff.

BACKGROUND OF THE TECHNOLOGY

2. RCN is an Internet service provider, or ISP, which is a company that provides access to the Internet and serves as a gateway to facilitate communications (of messages and other data) between a subscriber's computer and other computers and/or websites. Users of the Internet often navigate websites via a browser (e.g., Internet Explorer or Firefox). In doing so, customers type a web address, called a domain name (e.g., google.com), into the browser's address bar.[2] That domain name is sent to the ISP's server, which is a system (e.g., a computer, or some combination of software and hardware) that performs computer processing for the ISP. The ISP's server then uses a DNS ("Domain Name System") resolver, which acts like a phone book for the Internet, to translate the domain name (e.g., "google.com") into an IP address (like

[2] The "domain name" is the general reference to the website (e.g., "google.com" for Google), and forms part of a URL, or "Uniform Resource Locator." A URL is the unique, global address of each resource and file on the Web. A URL combines the domain name (e.g., google.com) with additional information like the protocol (e.g., http) or the path (information regarding the particular sub-part of the website). For example, the URL to reach Google's main search page is http://www.google.com. One of the URLs to reach Google's email service is http://www.google.com/mail (and "mail" is the "path" of the URL). Both of these URLs are at the same "domain name."

216.239.51.99). The DNS resolver serves a crucial purpose in directing an ISP customer to the website she wishes to view, not only because IP addresses for each website would be nearly impossible to remember, but also because IP addresses can change frequently.

3. When the user types in a web address (i.e., domain name or URL), the user's system asks the ISP's DNS resolver for the location of that website. The ISP should then return the "Internet address," i.e., IP address, that has been assigned to that domain name. Defendant RCN and the other ISPs use technology provided by Defendant Paxfire to give false answers to certain of customers' requests, and to send Plaintiff and the Classes to servers either owned or controlled by Defendant Paxfire, or to servers owned by the ISP and utilizing Paxfire's services (collectively, "Paxfire-based proxy servers").[3]

4. Researchers discovered this misconduct through use of a recently developed Internet tool called Netalyzr. Netalyzr is a publicly available network measurement, debugging, and diagnostic tool that evaluates the functionality provided by people's Internet connectivity. One of the primary focus areas of Netalyzr is DNS behavior. When users run the Netalyzr, the data gathered from the program is sent back to its developers. The creators of Netalyzr analyzed data from numerous tests and discovered cases of ISPs, including Defendant RCN, using DNS to redirect web searches to their own proxies.[4]

5. Netalyzr, available at http://netalyzr.icsi.berkeley.edu/, was developed by Nicholas Weaver, Christian Kreibich, and Vern Paxson, researchers affiliated with the

[3] Defendants redirect searches run via search.yahoo.com and www.bing.com through Paxfire servers. Searches run through www.google.com are not redirected by all ISPs; when Google searches are redirected, they are sometimes redirected through Paxfire servers, and sometimes redirected through ISP-located servers that utilize Paxfire technology.

[4] A "proxy" acts as an intermediary for requests from customers seeking resources from other servers.

International Computer Science Institute (ICSI) and the University of California, Berkeley. In the course of their investigation, Plaintiff's counsel consulted with the developers of Netalyzr regarding the technological aspects of the allegations in this complaint.

PARTIES

6. Plaintiff **Besty Feist** is an individual who resides in New York, NY. Plaintiff Feist is a paying customer of RCN, and uses RCN's services for Internet access, including to browse and/or search via Yahoo! (search.yahoo.com), Bing (www.bing.com), and Google (www.google.com). As discussed in detail below, Ms. Feist's searches were redirected to and intercepted by Defendants via Paxfire-based proxy servers.

7. Defendant **Paxfire, Inc.** ("Paxfire") is incorporated in Delaware, has corporate headquarters in Sterling, Virginia, and has offices worldwide. Defendant Paxfire works with ISPs throughout the United States. Defendant Paxfire claims to be the "proven industry leader in monetizing Address Bar Search and DNS Error traffic for Network Operators . . . [It] generate[s] millions of dollars a month in new advertising revenue for our partners by enabling them to participate in the booming $20 billion a year search advertising market."

8. Publicly, Defendant Paxfire provides its software and/or hardware to ISPs at no expense; redirects DNS errors (requests for mistyped web addresses or for websites that do not exist) to a site operated by Paxfire; and generates income via advertising on that site. Defendant Paxfire splits the revenue it generates with the ISPs, including Defendant RCN.

9. Surreptitiously, Defendant Paxfire also generates income for itself and the ISPs by intercepting searches run by the ISPs' customers and marketing the data derived from the interception to advertisers and marketers (by selling demographic data; modifying search results to including sponsored results; directing users to pages with paid advertisements on them; and/or

directing users to pages run by the advertisers and affiliates). This interception is not a publicly-stated revenue source for Defendant Paxfire, and is not a necessary function to allow ISPs to use Paxfire's DNS error redirection (i.e., internet service providers are able to use Paxfire for DNS error redirection without redirecting and/or intercepting search traffic).

10. Defendant **RCN Corporation** ("RCN") has its principle place of business in Herndon, Virginia, is incorporated in Delaware, and has subsidiaries organized and/or incorporated in Delaware, California, New York, Massachusetts, Pennsylvania, Illinois, and the District of Columbia. RCN is an ISP that employs Paxfire in connection with its domain name system ("DNS"). RCN provides Internet and phone service in and around Boston, Chicago, New York City, the Lehigh Valley of Pennsylvania, Philadelphia, and Washington, D.C.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and 1332(d), because the amount in controversy exceeds $5,000,000.00 exclusive of interests and costs, and there is at least minimal diversity between the members of the Classes and Defendants. This Court also has federal question jurisdiction as the complaint alleges violations of, *inter alia*, the Wiretap Act, 18 U.S.C. § 1510 *et seq.* This Court also has personal jurisdiction over Defendants because a substantial portion of the wrongdoing alleged took place in this state, Defendants conduct business in this state, and Defendants have sufficient minimum contacts with this state and/or otherwise intentionally availed themselves of the markets in this state through the promotion, marketing, sale, and use of their products and services in this state.

12. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391 as Plaintiff is a citizen and resident of this District, Defendants conduct business and have

significant contacts with this District, Defendant RCN has offices and subsidiaries located in this district, and a substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District.

FACTUAL ALLEGATIONS

Defendants Paxfire and RCN Redirect and Intercept Web Traffic

13. Defendant RCN installed Paxfire technology (either as software on its DNS servers or as physical hardware that sits before its DNS server) to monetize (i.e., generate revenue from) its customers' private searches. Publicly, Defendant Paxfire claims to monetize "DNS Error traffic," which occurs when an Internet user types in a domain name that does not exist or that contains a typo. In the case of a DNS Error, the user of an ISP that employs Paxfire is redirected to a Paxfire-created search results page, rather than being directed to an error page (e.g., "site not found").

14. However, as revealed by Netalyzr, Paxfire is also being used by the ISPs to intercept and monetize search data even when the user types in the correct address of an existing domain name *or* when the user is simply running a search. Paxfire (and the ISPs) can monetize user search data in a number of ways that fall into two major categories: monitoring and modification. Defendant RCN and Defendant Paxfire can monitor searches and market the data to advertisers and data aggregators interested in creating demographic profiles. Defendants can also modify the search data (e.g., prioritize the search results differently so as to eliminate certain websites or make others more prominent, or include sponsored/paid listings in the search results); can modify the advertisements that appear on the page to generate income from the traffic to the page; and can redirect the user completely, by sending him or her to an advertising affiliate's web page, rather than providing the requested search results.

How Defendants Redirect and Intercept Traffic

15. Defendant Paxfire intercepts, manipulates, and/or redirects traffic for three major search engines (google.com, bing.com, and search.yahoo.com (the "Search Engines")) in connection with various ISPs. Defendant RCN (using Paxfire technology) intercepts, manipulates, and/or redirects traffic for at least two of these Search Engines: bing.com and search.yahoo.com. One of the ways Defendants complete this interception is by redirecting customers' requests to a proxy server. When an RCN customer types in a web address (i.e., domain name or URL), the user's system asks the Defendant RCN's DNS resolver for the location of that website. However, when Defendants recognize a DNS request for one of the Search Engines, they provide an incorrect IP address, directing the customer to a Paxfire-based proxy server owned and controlled by Defendants. Defendants do this with no visible indication to Plaintiff or the Classes. Then, the customer's system connects to the IP address provided. (This entire procedure takes place in seconds or less).

16. While Plaintiff and the members of the Classes *think* they are communicating directly with one of the Search Engines, they are actually communicating with a server owned and controlled by Defendant Paxfire and/or Defendant RCN. Each time a customer enters a search into the Search Engine, the search goes to the Paxfire-based proxy server, which forwards the search to the Search Engine, then receives the search results on its own proxy server, and finally forwards the results back to the customer.

//

//

//

//

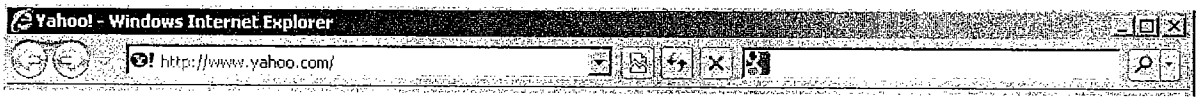
17. In other words:

SEARCH WEBSITE INTERCEPTION PROCESS	
What Should Happen:	**What Defendants Do:**
1. The user's system asks the ISP's DNS server for the address of one of the Search Engines.	1. The user's system asks the ISP's DNS server for address of one of the Search Engines.
2. The ISP returns to the user the IP Address designated for that Search Engine. Customer Request → ISP → Search Engine[5] Customer ← ISP ← Search Engine Address	2. The ISP returns to the user a false IP address, one that designates a server run by the ISP or by Paxfire. The Search Engine the user sought to connect with is not involved in any way. Customer request → ISP/Paxfire Customer ← Paxfire/ISP
3. The user's system then exchanges data directly with the server at the IP address provided-- the Search Engine. The user receives from that address the web page, which displays the search interface, and in turn the Search Engine transmits the results for the user's search terms. **Customer Search → Search Engine** **Customer ← Search Engine Results**	3. The user exchanges data with the proxy server at the ISP and/or Paxfire. At the same time, the ISP/Paxfire server makes its own connection to the true Search Engine server. The ISP/Paxfire server forwards to the Search Engine the user's text (although nothing prevents the ISP/Paxfire server from altering the search) and returns to the user's system the web page and results sent by the Search Engine (but again, nothing stops the ISP/Paxfire from changing the search results or web page). **Search → ISP/Paxfire → Search Engine** **Customer ← ISP/ Paxfire ← Search Results**

[5] This is a very simplified depiction of the lookup performed by the ISP in resolving the DNS (i.e., finding the appropriate IP address for the domain name), which is called "recursing." When "recursing," the ISP does not usually communicate directly with the Search Engine (or whatever website for which it may be trying to obtain an IP address). Instead, the ISP communicates with a series of servers, with increasingly narrow areas of information, until it reaches the server that holds the IP address for the requested site. For example, the ISP may seek which servers know about ".com" websites, and from there, find which server knows about sites at the "google.com" domain. When Paxfire is being used, however, the ISP does not do any recursion to locate the Search Engine's actual IP address. Instead, Paxfire, together with the ISP, unilaterally decide to return an IP address that belongs to either Paxfire, or a server at the ISP that uses Paxfire.

18. In either of the above examples—even when Paxfire was being used by the ISP to intercept searches—a customer would see an image of the Search Engine page, and would interact with the page as if communicating directly with the Search Engine. Even though Defendant RCN utilized Defendant Paxfire's technology to intercept searches, Plaintiff and the Classes would not know from viewing the website, running searches, or clicking links that they were actually being directed through the ISP's or Paxfire's server. Plaintiff and the Classes were never informed by Defendants that they were working together to provide incorrect DNS results; directing Defendant to their own servers for searches; impersonating the Search Engines; and gaining the ability to monitor, manipulate, and/or market Defendants' searches and search results.

19. Defendants also intercept and manipulate Plaintiff's searches by another means—the search bar. On many browsers, a search bar sits to the right of the address bar. Users can change the default search engine for this search bar, selecting, for example, Google, Yahoo!, or Bing. Below is a screen shot of the address bar, which shows that the user is currently visiting Yahoo!'s webpage (http://www.yahoo.com/), and the search bar, which shows (by the Google "g" logo) that the user has configured the search bar to use Google:



The search bar is visible to the user at all times, regardless of what web page the user is on.

20. RCN and Paxfire use this search bar to intercept and monetize searches for certain "brand keywords." The researchers at ICSI have identified approximately 170 brand keywords that, when used in searches, are not only intercepted by Defendants, but are forwarded on to a third-party advertising affiliate, who redirects the user to the brand's webpage. Instead of

receiving search results when a brand keyword is used as a search term, Defendants intercept Plaintiff's search, and a webpage for a particular brand is displayed.

21. For example, if class members search for "apple," they will not necessarily receive results for the term "apple," which may include links to Apple's website, information about Apple products, or information about the fruit, but may instead be directed to store.apple.com. (Searches for "mac," for which the first search result would typically be MAC Cosmetics, also direct class members to store.apple.com). Someone searching for "ca," for example, perhaps hoping to find information about California, will not receive such search results, but will be redirected to shop.ca.com, a website for CA Technologies which is a company that, ironically, sells "Internet security" software.

22. When the ISPs (including Defendant RCN) and Defendant Paxfire intercept searches made via a search bar, a similar process happens to that which occurs when a search is run (and intercepted) via Google's, Yahoo!'s, or Bing's search website:

SEARCH BAR INTERCEPTION PROCESS

- First, the user types a search term in the search bar.
- Then, the browser seeks the designated Search Engine's IP address from the ISP's DNS.
- Next, Defendants intercept that request and provide the user's system with an IP address to a Paxfire-based proxy server, rather than to the Search Engine's server.
- The Paxfire-based proxy server receives the search, and analyzes whether the search is coming from a search bar, or a search website.
- If the search is coming from a search bar, the Paxfire-based proxy server analyzes whether the search is for one of the 170+ brand keywords.
- If the search is coming from a search bar, but is *not* one of the brand keywords, the Paxfire-based proxy server will return search results, acting as a proxy server for the Search Engine, and displaying the Search Engine's webpage.[6]

[6] This step (occurring when the search is not for one of the brand keywords) parallels the "Search Website Interception Process" discussed above. Likewise, if the Paxfire-based proxy server

- If the search *is* one of the brand keywords, the Paxfire-based proxy server will send the search to an advertising affiliate that pays Defendant Paxfire (who splits the earnings with the ISPs, including Defendant RCN) for the referral.
- Finally, the advertising affiliate directs the user to the page associated with the brand keyword (i.e., displaying apple.com if the search term was "apple" or displaying dell.com if the search term was "dell").

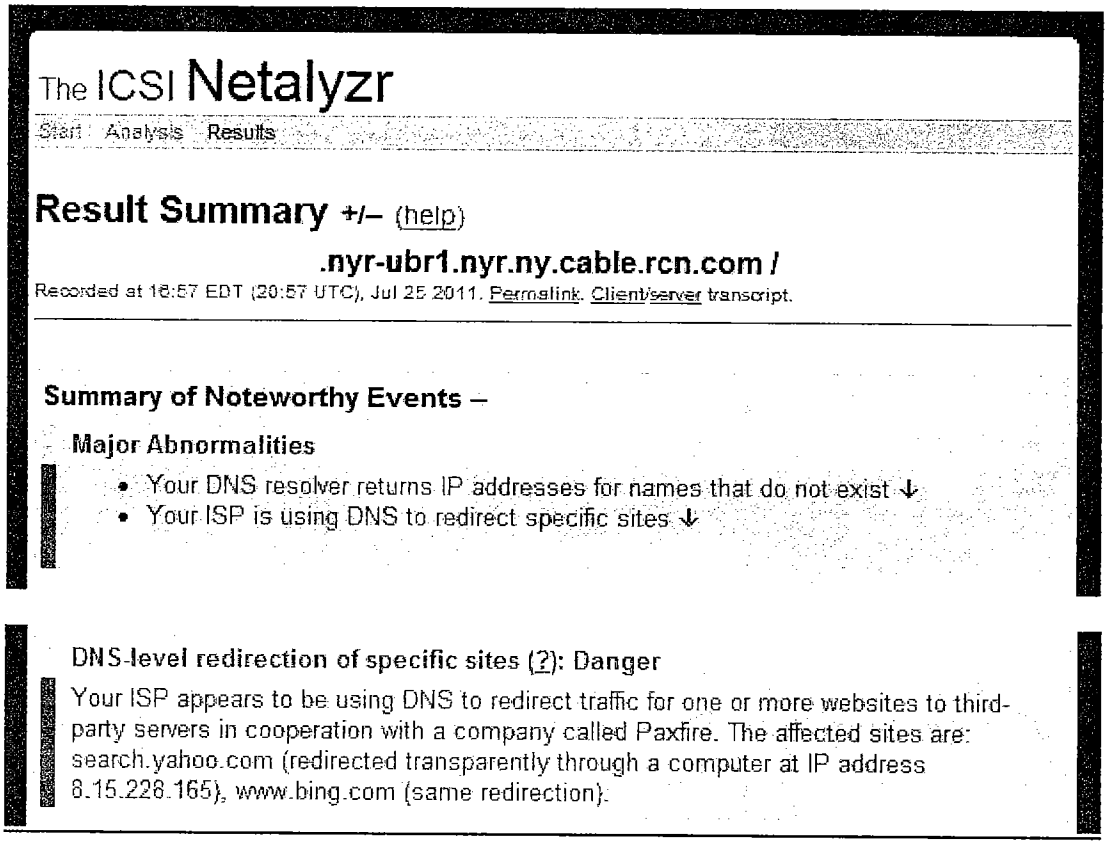
This entire process happens in less than a second, and is invisible to the user. Only very astute class members would even notice that they were being directed to a brand's page, rather than search results, when this process occurs.

[Remainder of Page Intentionally Left Blank]

---

determines that the search is not coming from a search bar, but from a search webpage, it follows the "Search Website Interception Process," and displays search results via a proxy server.

23. It was not until Plaintiff used Netalyzr that she learned that her ISP, Defendant RCN, was using Paxfire technology to redirect traffic that she had intended for the Search Engines to its own servers and/or those controlled by Defendant Paxfire. Plaintiff's Netalyzr results regarding DNS redirection appeared as follows:[7]



Defendants Profit From Their Deception at the Expense of Defendant RCN's Customers

24. This breach of Plaintiff's privacy and computer security is meaningful and problematic for numerous reasons, including, *inter alia*:

- it allows Defendant and Paxfire to receive, review, and compile the content of each of the user's searches, no matter how personal or private, and to share that information with and/or sell that information to third parties;

[7] Plaintiff's IP address has been redacted for privacy.

- it allows Defendant and Paxfire to manipulate Plaintiff's search terms, such that results she receives are altered;
- it allows Defendant and Paxfire to manipulate the web page returned to Plaintiff, by reordering and reprioritizing search results, eliminating search results, including paid and/or sponsored pages as search results, or altering advertising on the search page;
- it allows Defendant and Paxfire to send Plaintiff's private searches to a third-party advertising affiliate, earning money in the process, and directing Plaintiff to a brand's commercial webpage rather than to the search results she requested;
- it allows Defendant and Paxfire to know which websites the customer chooses among search results; and
- if the Plaintiff or a class member is logged in to a service connected with the Search Engine (e.g., searching on google.com while logged into Gmail, or searching on search.yahoo.com while logged into Yahoo! Mail), the customer's search history can be connected to his or her actual identity.

25. Not only is it profitable for RCN and Paxfire to intercept searches because it allows them to redirect traffic to advertisers and marketers who pay them for this information and/or increases traffic to their own pages, the demographic data and search history of customers, like Plaintiff, is itself tremendously valuable. By collecting personal information from computers and mobile devices, "[w]ebsites and stores can, therefore, easily buy and sell information on visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them." Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), *available at* http://ssrn.com/abstract=1478214. Multiple marketers have touted the high market value of this information in targeting consumers based on the data mined from their computers and mobile devices giving credence to the statement, "the more information that is known about a consumer, the more a company will pay to deliver a precisely-targeted advertisement to him." Federal Trade Commission Preliminary

Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change,* (Dec. 2010) at 24 ("FTC Report").

26. One data aggregator, Audience Science, states that its work involves "recording billions of behavioral events daily and reaching over 385 million unique Internet users" and then making such data available to its clients: "web publishers, marketers, networks, exchanges, and agencies[,] to create intelligent audience segments to connect people with relevant advertising driving the transition to data-driven audience marketing online." *See* MediaPost, http://www.mediapost.com/events/?/showID/OMMAGlobalNewYork.09.NewYorkCity/type/Exhibitor/itemID/647/OMMAGlobalNewYork-Exhibitors%20and%20Sponsors.html (last visited Aug. 3, 2011).

27. On March 7, 2011, the *Wall Street Journal* published an article under the headline, "Web's Hot New Commodity: Privacy" in which it highlighted a company called "Allow Ltd.," one of nearly a dozen companies that offer to sell people's personal information on their behalf, and giving them 70% of the sale. One Allow Ltd. customer received payment of $8.95 for letting Allow tell a credit-card company he is shopping for new credit. *Id.* In January 2011, at the World Economic Forum in Davos, Switzerland, one discussion centered on turning personal data into an "asset class." During the course of the discussion, Michele Luzi, director at consulting firm Bain & Co. stated, "We are trying to shift the focus from purely privacy to what we call property rights." *Id.*

28. Defendant RCN never disclosed to its customers that it shares their information with third parties, or that it allows third parties to access, monitor, or intercept customers' searches. Instead, RCN's current Customer Terms and Conditions include a "Customer Privacy Notice" which states, in relevant part:

> **At RCN, the privacy and security of your account is very important to us. That is why we have taken measures to protect the privacy of your personally identifiable account records and to comply with the federal laws and FCC regulations that govern use and disclosure of customer information.**
>
> * * *
>
> Internet privacy policies: RCN respects its subscribers' online privacy, and will not randomly monitor or disclose the contents of private e-mail or private chat room communications. However, as set forth fully in the RCN Internet Access Agreement, Customer agrees that RCN has the right, but not the obligation, to monitor or disclose the contents of private communication over the Internet, if RCN, in its sole discretion, reasonably believes that such action is necessary: (i) to comply with applicable law or valid legal process; (ii) to protect RCN rights or property; or (iii) in emergencies when a person's physical safety is at issue. In addition, RCN reserves the right to disclose the identity of a subscriber to third parties in response to a valid legal subpoena and to otherwise cooperate with legitimate law enforcement inquiries and lawful civil proceedings.

(Emphasis added).

29. RCN's "Online Policies" also state, in relevant part:

> RCN's dedication to customer service means that RCN strives to maintain an Internet Access Service ("Access Service") that provides RCN customers with an enjoyable Internet experience, and an experience that is **free from interference by persons who use the Access Service in an improper or unlawful manner.**

(Emphasis added).

30. Defendant RCN's purported privacy policies were untrue, misleading, incomplete, and deceptive, as they gave Plaintiff and members of the Classes a false sense that their information was being protected from unauthorized access to or interception by third parties or RCN itself, when in fact, Defendant RCN was actively accessing, intercepting, and manipulating its customers data, and allowing Defendant Paxfire to do the same.

31. Defendants failed to provide adequate notice to Plaintiff regarding the nature and use of Paxfire technology and failed to provide Plaintiff an adequate opportunity to opt out of the service.

32. Without Plaintiff's knowledge and/or consent, Defendant RCN knowingly and intentionally intercepted, monitored, marketed, and divulged to a third party Plaintiff's personal, private search history by intercepting and redirecting searches and impersonating Search Engines. In doing so, Defendant RCN breached numerous Federal and state laws that are designed to protect users' privacy, communications, and business dealings, as well as its privacy policies.

CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 on behalf of three classes, defined as follows: a) a class of persons who have had their Internet searches monitored, intercepted, altered and/or redirected via the use of Paxfire technology, including, but not limited to, the customers of the following Internet service providers: Cavalier, Charter, Cincinnati Bell, Cogent Communications, DirecPC, Frontier, Insight Broadband, Iowa Telecom, Defendant RCN, and Wide Open West, and any others to be determined in discovery (the "Paxfire Class"); b) a class of all RCN customers whose Internet searches were monitored, intercepted, altered and/or redirected (the "RCN Class"); and c) a class of all members of the RCN and/or Paxfire Classes who are citizens and/or residents of the state of New York (the "New York Class").

34. Excluded from the classes are Defendants; any parent, subsidiary, or affiliate of Defendants or any employees, officers, or directors of Defendants; legal representatives, successors, or assigns of Defendants; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

35. **Numerosity**. Each of the classes' members are so numerous and dispersed nationwide and/or statewide that joinder of all members is impracticable. Upon information and

belief, the classes' members number in the hundreds of thousands, if not millions. The exact number of members in each class is unknown, but can be determined from Defendants' computerized and other records. Plaintiff reasonably estimates and believes that there are thousands of persons in each of the classes.

36. **Commonality**. There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only individual class members. The members of the each class were and continue to be subjected to the same practices of the Defendants. The common questions and issues raised by Plaintiff's claims include:

(a) what information Paxfire's technology collected and what Defendants did with that information;

(b) whether class members received notice of the existence or use of Paxfire technology, and whether any such notice informed class members that their traffic would be misdirected and/or intercepted;

(c) whether consumers were provided an opportunity to decline the user of Paxfire technology;

(d) how Defendants monetized, i.e., generated revenue from, the information they monitored, intercepted, manipulated, and/or gathered;

(e) whether Defendant RCN breached its contracts, and if so, the appropriate measure of damages and remedies against Defendants for such breaches;

(f) whether Defendant RCN breached the covenants of good faith and fair dealing, and if so, the appropriate measure of damages and remedies against Defendants for such breach;

(g) whether Defendants RCN and/or Paxfire have violated the Wiretap Act, Virginia's Consumer Protection Act; New York General Business Law § 349; and other violations of common law;

(h) whether Plaintiff and the class members have been damaged as a result of Defendants' alleged violations as alleged herein; and, if so, the appropriate relief for Defendants' violations; and

(i) whether Defendants have been unjustly enriched as a result of their unlawful conduct, and, if so, whether Defendants should disgorge inequitably obtained money that they have been unjustly enriched by; and, the nature and extent of any other remedies, and injunctive relief, to which Plaintiff and the Classes are entitled.

37. **Typicality**. Plaintiff's claims are typical of the claims of all of the other members of the Class, because her claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendants.

38. **Adequacy**. Plaintiff will fairly and adequately protect the interests of all members of the class in the prosecution of this Action and in the administration of all matters relating to the claims stated herein. Plaintiff is similarly situated with, and has suffered similar injuries as, the members of the Class she seeks to represent. Plaintiff has retained counsel experienced in handling class action lawsuits. Neither Plaintiff nor her counsel have any interest that might cause them not to vigorously pursue this action.

39. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed.

Defendants have subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendants' uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendants acted and continue to act in a manner that is generally applicable to all members of the Class, making final injunctive relief appropriate.

COUNT I
Violation of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, against All Defendants

40. Plaintiff incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

41. Defendants intentionally intercepted, endeavored to intercept, and/or procured another person to intercept or endeavor to intercept a wire or electronic communication.

42. Defendants intentionally disclosed, or endeavored to disclose, to another person the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of the Wiretap Act.

43. Defendants intentionally used, or endeavored to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection.

44. Defendant RCN provided an electronic communication service to the public because it provides to its users the ability to send or receive wire communications (i.e., aural transfers made through the use of facilities for the transmission of communications by the aid of

wire, cable, or other like connection) and electronic communications. (i.e., the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire system that affects interstate or foreign commerce). In its capacity as an electronic communication service, Defendant RCN intentionally divulged the contents of its customers' communications while in transmission on its service to persons and entities other than an addressee or intended recipient of such communications.

45. Neither Defendant RCN nor Defendant Paxfire was an intended recipient of Plaintiff's communications, i.e., her searches.

46. The use of proxy servers was not necessary to the rendition of Defendant RCN's services.

47. Defendants engaged in the foregoing acts without obtaining the lawful consent of the user. Neither Defendant was an intended party of Plaintiff's communications with the Search Engines, and only gained access to those communications through their unlawful interception thereof. Defendant RCN thus could not have provided lawful consent to Defendant Paxfire to allow it to access or intercept Plaintiff's communications.

48. Plaintiff and the Class are entitled to equitable or declaratory relief; reasonable attorneys' fees and other litigation costs; punitive damages; and statutory damages which are the greater of (a) actual damages suffered plus any profits made by Defendants as a result of the violation and (b) statutory damages of $100 per day for each day of violation, with minimum statutory damages of $10,000.

COUNT II
Violation of Virginia's Consumer Protection Act, Virginia Code § 59.1 *et seq.*, against RCN
(On Behalf of the RCN Class)

49. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

50. This cause of action is brought pursuant to Virginia's Consumer Protection Act, Virginia Code § 59.1 *et seq.* (the "Act").

51. Defendant RCN's actions, representations and conduct have violated, and continue to violate the Act, because they extend to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers.

52. Plaintiff and other Class members engaged in "consumer transactions" as that term is defined by the Virginia Code § 59.1-198.

53. Defendant RCNs' Internet service that Plaintiff (and other similarly situated Class Members) purchased from Defendant RCN were "goods" and/or "services" within the meaning of Virginia Code § 59.1-198.

54. By engaging in the actions, representations and conduct set forth in this complaint, Defendant RCN has violated, and continues to violate, section 59.1-200(5) of the Act. Specifically, in violation of section 59.1-200(5), Defendant RCN misrepresented that its goods or services had certain quantities, characteristics, ingredients, uses, or benefits that they did not have.

55. By engaging in the actions, representations and conduct set forth in this complaint, Defendant RCN has violated, and continues to violate, section 59.1-200(6) of the Act. Specifically, in violation of section 59.1-200(6), Defendant RCN misrepresented that its goods or services were of a particular standard, quality, grade, style, or model when they were not.

56. By engaging in the actions, representations and conduct set forth in this Complaint, Defendant RCN has violated, and continues to violate, section 59.1-200(14) of the Act. Specifically, in violation of section 59.1-200(14), Defendant RCN's act and conduct constitute deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

57. Pursuant to § 59.1-204(A), Plaintiff, on behalf of herself and similarly situated Class members, seeks statutory damages in an amount of $500 per person. Plaintiff will also seek to have this amount increased to $1,000 per person at trial upon a showing of Defendant RCN's willful violation of the Act.

58. Plaintiff also requests that this Court award her costs and reasonable attorneys' fees pursuant to § 59.1-204(B).

59. Plaintiff further requests that this Court enjoin Defendant RCN from continuing to employ the unlawful methods, acts and practices alleged herein pursuant to the Act. If Defendant RCN is not restrained from engaging in these types of practices in the future, Plaintiff, Class members and other members of the general public will continue to suffer harm.

COUNT III
Violation of New York General Business Law § 349 against RCN
(On Behalf of the New York Class)

60. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

61. New York Gen. Bus. Law § 349 declares unlawful "deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this State." Gen. Bus. Law § 349(g) provides that § 349 "shall apply to all deceptive acts or practices declared to be unlawful, whether or not subject to any other law of this State."

62. Gen. Bus. Law § 349(h) provides a private right of action to any person injured by reason of a violation of that Section and authorizes the court to award reasonable attorney's fees to the prevailing plaintiff. In relevant part, it provides: "any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice and to recover her actual damages or $50, whichever is greater. The court may, in its discretion, increase the award of damages to an amount not to exceed three times the actual damages up to $1,000 if the court finds the defendant intentionally and knowingly violated this section. The court may award reasonable attorney's fees to a prevailing plaintiff."

63. Defendants, by their acts as alleged and described herein, have committed a violation of Gen. Bus. Law § 349 by disclosing Plaintiff's personal and confidential information without her knowledge or consent.

64. Defendants' acts and practices in the conduct of their businesses were deceptive and material.

65. Defendants, without authorization, disclosed Plaintiff's confidential and private information relating to Plaintiff's use of the Internet. Had she been given the choice, Plaintiff would not have disclosed her confidential and private information. Moreover, Plaintiff's confidential and private information is valuable personal property with a market value. As a result of Defendants' unlawful conduct, Plaintiff relinquished this valuable personal property without the compensation to which she was due.

COUNT IV
Conversion against All Defendants

66. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

67. Plaintiff's personal and private search history is valuable property owned by Plaintiff.

68. Defendants unlawfully exercised dominion over said property and thereby converted Plaintiff's and the Class members' respective personal information by providing it to third parties without authorization.

69. Plaintiff and the Class were damaged thereby.

COUNT V
Unjust Enrichment against All Defendants

70. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

71. By engaging in the conduct described in this complaint, Defendants have knowingly obtained benefits from Plaintiff under circumstances that make it inequitable and unjust for Defendants to retain them.

72. Defendants have received a benefit from Plaintiff and Defendants have received and retained money from third parties as a result of sharing and/or allowing access to the personal information of Plaintiff and Class members without Plaintiff's knowledge or consent as alleged in this complaint.

73. Plaintiff did not expect that Defendants would seek to gain commercial advantage from third parties by using and/or sharing her personal information without her consent.

74. Defendants knowingly used Plaintiff's personal information without her knowledge or consent to gain commercial advantage from third parties and had full knowledge of the benefits they have received from Plaintiff. If Plaintiff had known Defendants were accessing and/or not keeping her personal information from third parties, she would not have consented and Defendants would not have gained commercial advantage from third parties.

75. Defendants will be unjustly enriched if Defendants are permitted to retain the money paid to them by third parties, or resulting from the commercial advantage they gained, in exchange for Plaintiff's personal information.

76. Defendants should be required to provide restitution of all money obtained from their unlawful conduct.

77. Plaintiff and the members of the Class are entitled to an award of compensatory and punitive damages in an amount to be determined at trial or to the imposition of a constructive trust upon the wrongful revenues and/or profits obtained by and benefits conferred upon Defendants as a result of the wrongful actions as alleged in this complaint.

78. Plaintiff and the Class have no remedy at law to prevent Defendants from continuing the inequitable conduct alleged in this complaint and the continued unjust retention of the money Defendants received for the wrongful actions alleged in this complaint.

COUNT VIII
Breach of Contract against Defendant RCN
(On Behalf of the RCN Class)

79. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

80. Defendant RCN's Privacy Policy states that Defendant RCN "will not randomly monitor or disclose the contents of private e-mail or private chat room communications." Despite this promise, Defendant RCN did in fact knowingly share users' personal information with third parties in violation of its own agreement with its users.

81. Plaintiff never consented to the sharing of her personal information to third parties or with Defendant Paxfire.

82. Plaintiff has performed her obligations under the contract.

83. Defendant RCN materially breached its contractual obligations through its conduct as alleged herein, including intercepting Plaintiff's search requests, divulging Plaintiff's personal information and search requests to third parties, and impersonating and/or employing Paxfire in order to impersonate a Search Engine.

84. Plaintiff and the Class have been damaged as a direct and proximate result of Defendant RCN's breach of their agreements with Plaintiff and the Members of the Class.

COUNT IX
Breach of Implied Covenant of Good Faith and Fair Dealing against RCN
(On Behalf of the RCN Class)

85. Plaintiff hereby incorporates by reference the allegations contained in all of the preceding paragraphs of this complaint.

86. A covenant of good faith and fair dealing, which imposes upon each party to a contract a duty of good faith and fair dealing in its performance, is implied in every contract, including the agreement that embodies the relationship between Defendant RCN and its users.

87. Good faith and fair dealing is an element imposed by common law or statute as an element of every contract under the laws of every state. Under the covenant of good faith and fair dealing, both parties to a contract impliedly promise not to violate the spirit of the bargain and not to intentionally do anything to injure the other party's right to receive the benefits of the contract.

88. Plaintiff reasonably relied upon Defendant RCN to act in good faith, both with regard to the contract and in the methods and manner in which it carries out the contract terms. Bad faith can violate the spirit of the agreement and may be overt or may consist of inaction. Defendant RCN's inaction in failing to adequately notify Plaintiff of the release of personal information to outside advertisers and application developers evidences bad faith and ill motive.

89. The contract is a form contract, the terms of which Plaintiff is deemed to have accepted once Defendant RCN and the Class signed up with Defendant RCN. Defendant RCN is subject to an obligation to exercise its discretion regarding the contract, users' privacy, and the provision of Internet services in good faith. The covenant of good faith and fair dealing is breached when a party to a contract uses discretion conferred by the contract to act dishonestly or to act outside of accepted commercial practices. Defendant RCN breached its implied covenant of good faith and fair dealing by exercising bad faith in using its discretionary rights to deliberately, routinely, and systematically make Plaintiff's personal information available to third parties, access Plaintiff's personal information without consent, and impersonating (or allowing Paxfire to impersonate) a third party Search Engine.

90. Plaintiff has performed all, or substantially all, of the obligations imposed on her under the contract, whereas Defendant RCN has acted in a manner as to evade the spirit of the contract, in particular by deliberately, routinely, and systematically without notifying Plaintiff of its disclosure of her personal information to third-parties. Such actions represent a fundamental wrong that is clearly beyond the reasonable expectations of the parties. Defendant RCN's disclosure of an unauthorized access to Plaintiff's information is not in accordance with the reasonable expectations of the parties and evidences a dishonest purpose.

91. Defendant RCN's ill motive is further evidenced by its failure to obtain Plaintiff's consent to provide user information to Paxfire and/or impersonate a Search Engine to gain unauthorized access to users' data. Defendant RCN profits from revenues and traffic designed from this redirection and data mining.

92. The obligation imposed by the implied covenant of good faith and fair dealing is an obligation to refrain from opportunistic behavior. Defendant RCN has breached the implied

covenant of good faith and fair dealing in the agreement through its policies and practices as alleged herein. Plaintiff and the Class have sustained damages and seek a determination that the policies and procedures of Defendant RCN are not consonant with Defendant RCN's implied duties of good faith and fair dealing.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, requests the following relief:

A. An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiff be appointed as Class Representative, and that Plaintiff's counsel be appointed Class Counsel;

B. An award of damages;

C. Restitution of all monies unjustly obtained or to be obtained from Plaintiff and members of the Class;

D. Declaratory and injunctive relief;

E. An award of reasonable attorneys' fees and costs; and

F. Such other relief at law or equity as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial of her claims by jury to the extent authorized by law.

Dated: August 4, 2011

Respectfully Submitted,

MILBERG LLP

Sanford P. Dumain
Peter E. Seidman
Melissa Ryan Clark
Charles Slidders
One Pennsylvania Plaza, 49th Floor
New York, NY 10119
Telephone: (212) 594-5300

Facsimile: (212) 868-1229
E-mail:sdumain@milberg.com
pseidman@milberg.com
mclark@milberg.com
cslidders@milberg.com

-and-

REESE RICHMAN LLP
Michael E. Reese
Kim Richman
875 Avenue of the Americas, 18th Floor
New York, NY 10001
Telephone: (212) 579-4625
Facsimile: (212) 253-4272
E-mail: mreese@reeserichman.com
krichman@reeserichman.com

Attorneys for Plaintiff Betsy Feist